The Facebook, Inc. v. Connectu, LLC et al Doc. 251

G. HOPKINS GUY, III (State Bar No. 124811)
hopguy@orrick.com
I. NEEL CHATTERJEE (State Bar No. 173985)
nchatterjee@orrick.com
MONTE COOPER (State Bar No. 196746)
mcooper@orrick.com
THERESA A. SUTTON (State Bar No. 211857)
tsutton@orrick.com
YVONNE P. GREER (State Bar No. 214072)
ygreer@orrick.com
ORRICK, HERRINGTON & SUTCLIFFE LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: 650-614-7400
Facsimile: 650-614-7401

Attorneys for Plaintiffs
THE FACEBOOK, INC. and MARK ZUCKERBERG

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

THE FACEBOOK, INC. and MARK ZUCKERBERG,

Plaintiffs,

v.

CONNECTU, INC. (formerly known as CONNECTU, LLC), PACIFIC NORTHWEST SOFTWARE, INC., WINSTON WILLIAMS, WAYNE CHANG, and DAVID GUCWA,

Defendants.

Case No. 5:07-CV-01389-RS

REDACTED/PUBLIC VERSION OF:

PLAINTIFFS' MOTION FOR PARTIAL SUMMARY JUDGMENT RE DEFENDANTS' LIABILITY PURSUANT TO CALIFORNIA PENAL CODE SECTION 502(C) AND 15 U.S.C. § 7704(A)(1) AND 15 U.S.C. § 7704(B)(1)

Date: February 13, 2008
Time: 9:30 A.M.
Judge: Honorable Richard Seeborg

Dockets.Justia.com

TABLE OF CONTENTS

				Page
I.	INTRODUCTION			1
II.	FACTUAL BACKGROUND			1
	A.	The Facebook Computer System and Website		1
	B.	Facebook's Terms of Use Dictate Authorized Access to Its Website		2
	C.	ConnectU's Unauthorized Access of the Facebook Site in 2004 to Obtain Email Addresses and Course Information of Facebook's Registered Users		3
	D.	ConnectU's Unauthorized Harvesting and Spamming Activities in 2004		4
	E.	Defendants' Use of "Importer" to Harvest Email Addresses and Profile Information of Facebook's Registered Users		6
	F.	Defendants Use the Harvested Emails to Send Unsolicited Commercial Messages to Facebook Users		9
	G.	Defendants Did Not Have Permission to Access Plaintiffs' Computers Via Importer to Take or Use Data Available from Facebook's Website		11
	H.	Plaintiffs Suffer Loss and Harm by Defendants' Unauthorized Access of the Facebook Website		12
III.	ARGUMENT			15
	A.	Legal Standard		15
	B.	Defendants Have Violated California Penal Code § 502(c)		15
		1.	Plaintiffs' Computers Are Covered By Penal Code Section 502(c)	16
		2.	Defendants Knowingly and Without Permission Accessed or Caused to be Accessed Facebook's Computer System	17
		3.	Defendants Admit that They Took, Copied and/or Made Use of Facebook's Data	18
	C.	ConnectU and PNS Violated 15 U.S.C. § 7704(a)(1)		19
		1.	Defendants' Email Messages Are "Commercial" Electronic Mail Messages	19
		2.	ConnectU and PNS "Initiated" the Transmission of the Emails	20
		3.	The Emails Sent by PNS and ConnectU Had False Headers	21
		4.	Defendants' Actions Constitute an Aggravated Violation Allowing for Trebling	22
			a. ConnectU and PNS's Actions Were Willful and Knowing	22
			b. ConnectU and PNS' Automated Harvesting Violated Section 7704(b)(1)	23
	D.	Facebook and Zuckerberg Were Adversely Affected		24
IV.	CONCLUSION			25

TABLE OF AUTHORITIES

Page

FEDERAL CASES

Aitken v. *Commc'n Workers of America*, 496 F. Supp. 2d 653 (E.D. Va. 2007) 19, 21, 22

Celotex Corp. v. *Catrett*, 477 U.S. 317 (1986) 15

Facebook, Inc. v. *ConnectU LLC*, 489 F. Supp. 2d 1087 (N.D. Cal. 2007) 17, 18

MySpace, Inc. v. *Wallac.*, 498 F. Supp. 2d 1293 (C.D. Cal. 2007) 19

United States v. *Middleton*, 231 F.3d 1207 (9th Cir. 2000) 17

FEDERAL STATUTES

70 Fed. Reg. at 3315 22

15 U.S.C. §7702(2) 19

15 U.S.C. § 7702(6) 19

15 U.S.C. § 7702(9) 20

15 U.S.C. § 7704(a)(5)(A) 19

15 U.S.C. § 7704(b)(1) 11, 22

15 U.S.C. § 7704(b)(1)(A)(i) 12

15 U.S.C. § 7706(g)(1) 12

15 U.S.C. § 7706(g)(2) 20

16 C.F.R. 316(3) 19

15 U.S.C. § 7704(a)(1) 11, 13, 19, 20, 21, 22

STATE STATUTES

Cal. Penal Code § 502(a) 16

Cal. Penal Code § 502(b)(2), (4),(5) 16

Cal. Penal Code § 502(b)(9) 17

Cal. Penal Code § 502(c) 15, 16, 18

Cal. Penal Code § 502(e)(1) 16

Cal. Penal Code § 502(e)(4) 16

I. INTRODUCTION

Plaintiffs request partial summary judgment finding liability in their favor as follows:

1. All Defendants violated California Penal Code § 502(c); and
2. Defendants ConnectU, Inc. and Pacific Northwest Software, Inc. violated the CAN-SPAM Act, 15 U.S.C. §§ 7704(a)(1).

With the entry of partial summary judgment, the only remaining issues will be damages on the Penal Code § 502(c) and CAN-SPAM claims, and liability with respect to the California and Massachusetts common law misappropriation claims, the claim for violation of the Computer Fraud and Abuse Act, and the Massachusetts Unfair Trade Practices Act.

The following facts are not in dispute. The Defendants intentionally and willfully hacked into the Facebook website to harvest millions of bits of data, including email addresses, using manual and automated processes. On many occasions, the Defendants conducted their hacking campaign in a way designed to avoid detection. They then sent emails with false headers to the stolen email addresses. Even when Facebook erected numerous barriers to halt Defendants' attack and Defendants were told their actions were unlawful, the Defendants continued. Defendants did not have authorization to do what they did. Defendants violated the law.

II. FACTUAL BACKGROUND

There is no disputed issue of material fact that (a) Facebook is a computer system that uses numerous servers in order to run the popular social network www.facebook.com; (b) Defendants personally logged into the Facebook website using user identifications and passwords that did not belong to them and also developed automated computer programs to log into the Facebook website; (c) Defendants knowingly accessed the Facebook website and without permission copied and made use of data, including email addresses, from the Facebook website; (d) Defendants used the harvested information to send unsolicited commercial email with false and/or misleading header information to Facebook users; and (e) plaintiffs engaged in substantial efforts to stop the harmful attacks.

A. The Facebook Computer System and Website

Facebook is a social network website that launched on February 4, 2004 as "www.thefacebook.com." Declaration of Monte M.F. Cooper in Support of Plaintiffs' Motion for Partial Summary Judgment ("Cooper Decl.") Ex. 1 at 119:6-123:19. Since its very beginning, the Facebook website has used collections of servers that store information and execute a variety of software programs that enable the website to function. *Id.* at 84:21-25, 146:5-19, 155:2-156:7; Ex. 2 at 232:19-22, 247:1-250:2; Ex. 3; Ex. 4. As of August 9, 2004, the servers used to host the website were located in California. *Id.* Ex 1 at 165:13-166:4; Ex. 5. By March 2006, Facebook employed between 500 and 600 servers as part of this computer system. *Id.* Ex. 1 at 180:24-181:2; Ex. 2; Exs. 3 - 4. Facebook's founder Mark Zuckerberg originally operated the Facebook website while he was a student at Harvard, but in June 2004 he re-located its operations to Silicon Valley during his summer break. Facebook, Inc. was later incorporated into a business to operate the Facebook website. *Id.* Ex. 1 at 93:13-94:10. 193:6-11.

B. Facebook's Terms of Use Dictate Authorized Access to Its Website

Since its introduction on February 4, 2004, Facebook's popularity has steadily grown. By July 1, 2005, Facebook's website had 3 million registered users, many of them students at California schools. *Id.* Ex. 1 at 245:22-246:12; Zuckerberg Decl., ¶ 2.

Every Facebook user agrees to conditions that govern the use of the Facebook website. Cooper Decl. Ex. 1 at 238:11-16, 238:22-25, 238:18-239:5; Zuckerberg Decl. ¶ 3-4. For example, between February 4, 2004 and August 17, 2005, an individual registering to use Facebook was required to provide a college or university email address. Cooper Decl. Ex. 1 at 120:12-20. To complete the registration process, the user also agreed to be bound by the "Terms of Use," governing access to the website. *Id.* Ex. 1 at 238:11-16, 238:22-25, 238:18-239:5; Zuckerberg Decl. ¶ 4. Facebook's Terms of Use conditioned an individual's access to the site upon the user's agreement (a) not to use the site for commercial endeavors, (b) to refrain from the "harvesting" of email addresses and other profile information of registered users, and (c) not to use information for the solicitation (*i.e.*, "spamming") of Facebook members. Zuckerberg Decl. ¶¶ 4-7 & Exs. A-C. Facebook's Terms of Use as of September 19, 2004 is representative, and read in pertinent part:

> The Web site is for the personal use of individual Members only

> and may not be used in connection with any commercial endeavors. Organizations, companies, and/or businesses may not become Members and should not use the Service or the Web site for any purpose. Illegal and/or unauthorized uses of the Web site, including collecting email addresses or other contact information of members by electronic or other means for the purpose of sending unsolicited email and unauthorized framing of or linking to the Web site will be investigated, and appropriate legal action will be taken, including without limitation, civil, criminal, and injunctive redress.

Id. Ex. B. Between February 4, 2004 and August 2005, Facebook's Privacy Policy also specified that "Email addresses will never be sold to anyone, and they will not be used for spam or any other purpose outside of the site itself." *Id.* ¶ 8 & Exs. D-E. After registering and agreeing to these Terms of Use, a user of the Facebook computer system was permitted to communicate electronically with other Facebook members and have access to view the personal data of other users within his or her particular college network (*i.e.*, other students and alumni). Cooper Decl., Ex. 1 at 129:14-134:9; Zuckerberg Decl. ¶¶ 4, 9 & Exs. A-C. By at least May 4, 2004, ConnectU had specifically visited Facebook's registration page, where its Terms of Use was presented. Zuckerberg Decl. ¶ 4; Cooper Decl. Ex. 6; Ex. 7 at 31:23-32:2. Plaintiffs have never authorized anyone affiliated with ConnectU to access the Facebook website to extract, copy, or use any information on the Facebook website for ConnectU-related purposes. Zuckerberg Decl. ¶ 10.

A fundamental aspect of the Facebook website from its creation was its privacy features. Cooper Decl. Ex. 1 at 83:6-12, 122:23-124:19, 124:20-125:25, 238:18-239:5. Specifically, the information about particular users was not made accessible to all users. *Id.* Rather, only approved "friends" or other users within the same network (*e.g.*, Harvard College) could review a particular user's profile, and even then only when privacy settings allowed such viewing. *Id.*

C. ConnectU's Unauthorized Access of the Facebook Site in 2004 to Obtain Email Addresses and Course Information of Facebook's Registered Users

ConnectU was formed in 2004 by Harvard students Cameron Winklevoss, Tyler Winklevoss and Divya Narendra ("the ConnectU Founders"). Cooper Decl. Ex. 8, Response to Interrogatory No. 7 . ConnectU operates the social network website www.connectu.com, which competes with Facebook. *Id.* Ex. 9 at GUCWA 0124 (15:21:06–15:21:41).

[redacted] Cooper Decl. Ex. 10 at 43:12-44:5, 45:17-46:3, 53:6-20; Ex. 11 at 72:17-73:11, 73:19-22, 73:25-74:7; Ex. 7 at 24:10-28:1; Ex. 12 at 31:2-11, 53:22-54:24. ConnectU's founders each admitted that they "personally downloaded onto [their] computer[s] some of these email addresses [they] found on thefacebook.com." *Id.* Exs. 13-15 at ¶ 2 (bracketing added). ConnectU and its Founders also have confirmed that all such actions, as well as downloading, were done on behalf of ConnectU. *Id.* Exs. 16-18, Responses to Form Interrogatories Nos. 2.11 & 8.2; Ex. 19, Response to Form Interrogatory No. 17.1 at 4-5 (Requests Nos. 2, 9, 10 & 12).

ConnectU's purpose was admittedly and expressly commercial. [redacted] *Id.* Ex. 10 at 53:14-20. As early as May 3, 2004, Founder Cameron Winklevoss bragged to his father that "[w]e have also been able to suck courses of [sic] thefacebook.com…." *Id.* Ex. 20 at C003868. Cameron Winklevoss further acknowledged that while Facebook "spent 100s of hours over the last 3 months collecting them [the course information]," "we will essentially be getting them fast and free." *Id.*

D. ConnectU's Unauthorized Harvesting and Spamming Activities in 2004

At some point during the illegal hacking and harvesting activities, ConnectU decided that manually downloading email addresses was too cumbersome and decided to automate the process. ConnectU's Founders hired iMarc LLC, a website developer, to help build the ConnectU website based on the "look and feel of" Facebook and other social networking websites. Cooper Decl. Ex. 11 at 30:21-31:9; Ex. 21 at 23:16-27:21, 48:19-50:1. Initially, iMarc hosted the ConnectU website on its own servers. *Id.* Ex. 21 at 66:4-25, 118:25-121:3, 158:15-159:21 [1] In the summer of 2004, iMarc was asked by ConnectU to engage in "screen-scraping"

[1] iMarc authenticated all emails sent from any of its members, including David Tufts, Nils Menton, Marc Pierrat, Bill Bushee, Nick Grant, and Fred LeBlanc. Cooper Decl. Ex. 21 at 7:20-21, 14:8-11, 15:12-16:10, 20:2-23:11.

(*i.e.* harvesting) of email addresses and spamming of Facebook users. Specifically, on or around June 11, 2004, ConnectU asked iMarc to:

> [W]rite a little script that logs into www.thefacebook.com, loops through http: //www. thefacebook.com/profile.php?id=xxxxx replacing xxxxx with numbers to grab people's email addresses.

Id. Ex. 22; Ex. 21 at 128:13-132:23, 133:7-135:13. iMarc refused to write such a program because it was "unethical" and might expose it to liability. *Id.* Ex. 21 at 66:4-68:25, 124:23-125:17, 128:13-147:4, 149:9-150:6, 153:13-22, 156:5-157:21; Exs. 23-27.

Because iMarc refused to assist in ConnectU's "hack and spam" campaign, ConnectU went elsewhere. For instance, ConnectU sought the assistance of Deva Mishra, a friend of Founder Divya Narendra. Deva Mishra was asked to write the script iMarc refused to write. Mr. Mishra contacted iMarc and said he was writing the requested script for ConnectU. *Id.* Ex. 25; Ex. 28 at 191:5-192:14; Ex. 21 at 136:12-140:13. iMarc never responded to Mr. Mishra's email. *Id.* Ex. 21 at 139:21-22.

On July 22, 2004, ConnectU sent thousands of unsolicited emails from "bogus" college accounts to students, at least some of whose email addresses were garnered from Facebook, inviting them to join ConnectU. *Id.* Ex. 26; Ex. 19, Response to Form Interrogatory 17.1 at 5 (Request No. 8); Ex. 21 at 140:14-147:4. The "from" lines used email address headers such as "god@harvard.edu" and three email addresses from different universities all using the same name "jstarr." *Id.* Ex. 26. An agent of ConnectU later confirmed that "jstarr" is a "fake" email address. *Id.* Ex. 29. "jstarr" was admittedly a fictitious name. *Id.* As a result of these actions, iMarc quickly terminated its hosting of the ConnectU website. *Id.* Ex. 21 at 66:4-68:25, 163:13-164:11. The website was transferred to another location. *Id.* Despite the transfer, iMarc continued to receive complaints concerning ConnectU's spamming as late as September 2004, and on August 26, 2004, an iMarc representative specifically advised ConnectU that it should be concerned that such spamming activities could result in ConnectU's being blacklisted and "sued for damages" for violating the Federal CAN-SPAM Act. *Id.* Ex. 29; Ex. 27; Ex. 21 at 152:16-154:2, 156:5-157:21. Nonetheless, ConnectU continued its "hack and spam" campaign.

E. Defendants' Use of "Importer" to Harvest Email Addresses and Profile Information of Facebook's Registered Users

In late 2004 or early 2005, ConnectU hired Defendants Pacific Northwest Software ("PNS") and Winston Williams to continue development of the ConnectU site and to "work with some email addresses that ConnectU obtained from Plaintiff's website." *Id.* Ex. 19, Response to Form Interrogatory 17.1 at 5-6 (Request Nos. 12-13); Ex. 30 at 19:14-20:9; Ex. 11 at 82:2-83:2. Williams, along with Defendants Wayne Chang and David Gucwa, and PNS employee Joel Voss, helped develop computer programs known as the "Facebook Importer" and "Crawler" as part of a service they labeled "Social Butterfly." *Id.* Ex. 31 at 57:24-60:2, 72:2-73:20, 86:8-89:14, 165:12-17, 167:22-168:3; Ex. 30 at 27:24-28:6, 98:2-99:3, 104:5-8, 106:13-18, 172:4-16; Ex. 32; Ex. 33; Ex. 34 at PNS000015; Ex. 35 at 148:20-151:6, 29:17-31:23; Ex. 11 at 83:22-84:23, 85:10-87:22; Ex. 36.

Defendants used these programs to "grab data from the Facebook Website," including "extracting" email addresses of Facebook's users. Cooper Decl. Ex. 9 at GUCWA 0022 (15:03:25-15:18:15), GUCWA 0023 (16:07:43-16:09:10), GUCWA 0024 (16:10:36-16:10:39, 17:20:19-17:23:16), GUCWA 0032-33 (13:23:54-13:28:03), GUCWA 0048 (11:29:48-11:33:49), GUCWA 0057 (12:02:53-12:06:49), GUCWA 0060 (14:18:05-14:20:3), GUCWA 0071 (12:36:24-12:39:04), GUCWA 0075-78 (16:44:12–18:54:46), GUCWA 0142 (18:42:42-19:11:43); Ex. 36; Ex. 31 at 208:16-209:20, 211:17-212:15; Ex. 35 at 148:20-151:6, 29:17-31:23; Ex. 11 at 83:22-87:22; Declaration of Chris Shiflett in Support of Plaintiff's Motion for Partial Summary Judgment ("Shiflett Decl.") ¶¶ 10, 15-16. Many of the features of the software are described in time and date-stamped AOL instant messages produced by Gucwa reflecting his conversations with co-Defendants Chang (identified as "dr ttol" or "wayneati2hub"), Williams (identified as "Winston" or "rrrmrprim8"), PNS' President John Taves (identified as "JTpickAtime"), PNS employee Joel Voss (identified as "Javantea1"), and ConnectU Founders Cameron and Tyler Winklevoss (identified as "CWinklevoss" and "TWinklevoss," respectively). Cooper Decl., Ex. 31 at 207:2-7, 208:16-25; Ex. 9 at GUCWA 0003 (18:40:17-18:43:10), GUCWA 0009 (12:47:14-12:51:11), GUCWA 0128 (15:16:46-15:17:02), GUCWA 0130

(17:43:52), GUCWA 0152-153 (21:46:59-21:47:29, 21:50:43-47, 22:10:38-22:11:36). The architecture of these combined tools was set out in a document authored by Defendants, and is illustrated (with annotations added by Facebook to explain the functions) as follows:

See id. Ex. 36. Particular features of this architecture are reflected in source code produced by the Defendants. *See generally* Shiflett Decl. ¶¶ 10-14 & Exs. 4-6. The Defendants described their software as a "social network spider." Cooper Decl. Ex. 9 at GUCWA 0057 (12:02:53-12:06:49), GUCWA 0058-0059 (12:45:15-13:50:47).

As reflected by the architectural diagram, the code and Defendants' own discussions, Defendants would use a log-in account and password supplied by ConnectU. *Id.* Ex. 9 at GUCWA 0022 (15:04:44-15:17:39), GUCWA 0025 (18:28:31-18:44:27), GUCWA 0032-33 (13:23:54-13:28:03), GUCWA 0075-77 (17:28:27-18:19:07); Ex. 36. *See also* Shiflett Decl. ¶¶ 10, 11, 15, 34 & Ex. 4. The tool would then access all profiles viewable by that user. Cooper Decl. Ex. 9 at GUCWA 0058 (12:45:43-12:47:17, 13:10:14-13:21:07); Shiflett Decl. ¶ 15. For example, if the log-in was from Harvard, all Harvard profiles would be reviewed. Cooper Decl. Ex. 9 at GUCWA 0058 (12:59:42-43) ("at least we can index schools . . . with just one email"); *see also id.* at GUCWA 0073-0078 (13:49:32-18:54:46).[2] In addition, all profiles of the "friends" of the log-in account owner associated with other schools would also be reviewed. *Id.* at GUCWA 0060 (14:11:07-14:19:10); Shiflett Decl. ¶¶ 15-16 & Ex. 4 at PNS0281502 [redacted]

This practice was called "crawling" and "spidering." Cooper Decl. Ex. 9 at GUCWA 0057 (12:06:49-12:07:48), GUCWA 0060 (14:11:07-14:12:30); Shiflett Decl. ¶ 11 n.4. The tool copied the email addresses and other profile information that were located by the "crawl" or "spider." *Id.* The data copied from the Facebook website was stored in ConnectU's database via a program that would "grab email addresses from the friends listed on that account." Cooper Decl. Ex. 9 at GUCWA 0057 (12:02:53-12:04:08); Shiflett Decl. ¶¶ 15-16. Once in the database, ConnectU would "send out an invite email" and "add the email to a master database." *Id.* Ex. 9 at GUCWA 0057 (12:04:52-12:06:49); Shiflett Decl. ¶¶ 17-19.[3] Nothing in the code indicates that

[2] While Defendants have admitted that their code accessed and scraped the email addresses for an entire school using one Facebook login from that school, Defendants have not produced the relevant code associated with this functionality.

[3] ConnectU permitted its users to voluntarily "import" Facebook profile information. This importation violated Facebook's Terms of Use to the extent it harvested email addresses. More importantly, though, ConnectU did not disclose to its users that even this "importing" function would automatically send invitation emails to the friends' addresses that were imported. Cooper Decl. Ex. 37. Indeed, ConnectU's own privacy policy said email addresses it obtained would not be used for spam. *Id.* Ex. 38. In any event, the evidence reflects that ConnectU sent unsolicited invitations to email addresses originally obtained using the automated "spider" reflected in the source code. *See, e.g.*, Cooper Decl. Ex. 40; Shiflett Decl. ¶¶ 15-19 & Exs. 4-6.

a ConnectU user's authentication was needed to send the invitations. Shiflett Decl. ¶ 18.

Defendants expected that using just 300 login registrations (one for each school) they could "access 1 mil profiles." Cooper Decl. Ex. 9 at GUCWA 0058 (12:59:42-13:01:03). [redacted] *Id.* Ex. 32 at PNS01768 (3/9/05 entry), PNS01769 (4/6/05 entry); Shiflett Decl. ¶¶ 15-16 & Ex. 4 at PNS0281469-73, Ex. 6 at PNS0310177. [redacted] Cooper Decl. Ex. 32 at PNS01769 (4/7/05 entry). ConnectU admits that Defendants extracted at least 2.9 to 3 million email addresses from the Facebook website for use in sending commercial e-mails. *Id.* Ex. 35 at 148:20-150:16; Ex. 11 at 83:22-84:23, 85:10-87:22.[4]

F. Defendants Use the Harvested Emails to Send Unsolicited Commercial Messages to Facebook Users

Using the imported email addresses from Facebook that had been grabbed and scanned, Defendants employed "Social Butterfly" as a means to send invitations to Facebook's registered users to join ConnectU. *Id.* Ex. 35 at 148:20-150:16; Ex. 31 at 126:8-127:25; Ex. 36; Ex. 9 at GUCWA 0057 (12:02:45-12:06:49); Ex. 41 at PNS01380-83; Ex. 42; Shiflett Decl. ¶¶ 17-19. The invitations were sent solely to encourage Facebook users to join the competing ConnectU commercial service. The emails sent by Defendants contained the following content advertising for ConnectU or similar messages:

[redacted]

[redacted]

See Cooper Decl. Ex. 43; Ex. 40; Ex. 63; Ex. 64.

---

[4] The actual number of email addresses obtained by Defendants from Facebook, and the number of invitations sent by Defendants to Facebook users soliciting them to join ConnectU, remains unclear because Defendants refuse to produce this information. *See* Cooper Decl. Exs. 65-66. [redacted] Id. Ex. 42.

These email invitations misleadingly suggested that they were produced by Facebook users, but actually were sent by PNS and ConnectU. *Id.* Ex. 9 at GUCWA 0060 (14:20:20-14:20:30); Ex. 40; Ex. 43; Ex. 63; Ex. 64; Ex. 44 (Response to Interrogatory No. 4); Shiflett Decl. ¶¶ 17-19. The following is an example of the header information in an e-mail generated by Defendants' software programs:

[redacted]

Cooper Decl. Ex. 43; *see also id.* Ex. 40; Ex. 63; Ex. 64; Ex. 1 at 241:8-242:24. [redacted] *Id.* Ex. 43; *see also id.* Ex. 40; Ex. 63; Ex. 64. [redacted] *Id. See also id.* Ex. 9 at GUCWA 0060 (14:20:20-14:20:30). [redacted] *See* Shiflett Decl. ¶¶ 17-18 & Ex. 6 at PNS0310177. [redacted] *See, e.g.,* Cooper Decl. Ex. 40; Ex. 43. [redacted] *Id.*

Defendants knew these spam emails employed misleading headers and were causing complaints from Facebook users, as evidenced by the following instant message discussion between ConnectU Founder Tyler Winklevoss and David Gucwa:

> (22:10:55) David Gucwa: we've gotten complaints from people about spamming them
>
> (22:10:57) TWinklevoss: winston said it have [sic] something to do with how the headers worked
>
> (22:11:00) David Gucwa: oh
>
> (22:11:02) TWinklevoss: from who?
>
> (22:11:16) David Gucwa: I don't know, some person from

thefacebook

(22:11:25) David Gucwa: I got a forwarded email about it

(22:11:29) David Gucwa: from cameron I think

(22:11:36) TWinklevoss: ok

Id. Ex. 9 at GUCWA 0153 (22:10:55-22:11:36).

G. Defendants Did Not Have Permission to Access Plaintiffs' Computers Via Importer to Take or Use Data Available from Facebook's Website

Defendants knew that their efforts to acquire email addresses and then spam Facebook's users were undertaken without Facebook's permission. [redacted] *Id.* Ex. 34 at PNS000015 (emphasis added). Likewise, when originally developing their scripts, Defendants acknowledged that "we don't want thefacebook and other sites to be able to easily shut off the importer," and instead "we'd [Defendants] rather play cat and mouse than have them just firewall us off." *Id.* Ex. 9 at GUCWA 0049 (17:01:22-17:01:25). For that reason, Defendants also admitted in conversations with one another that "once thefacebook finds out they will try to mangle things to shut out our script so [Defendants] will have to play cut [sic, cat] and mouse [and] modularize the login sequence and the retrieval of fields[,] etc." *Id.* at GUCWA 0023 (16:07:41-16:09:10).

In fact, during Defendants' initial use of Importer on January 27, 2005, Chang commented "we're prob [sic, probably] setting up huge alarms at thefacebook[,] how can we go faster"? *Id.* at GUCWA 0076 (17:57:19-17:57:30). [redacted] *Id.* Ex. 45. [redacted] *Id.* [redacted]

[redacted] *Id.* Ex. 46.

Defendants appreciated the wrongfulness of their actions, as they tried to avoid detection. [redacted] *Id.* Ex. 47. Defendants also took measures to prevent Facebook from realizing they were seeking to obtain data such as email addresses from Facebook's website (discussed below), because they were concerned that "once thefacebook finds out" Facebook would "shut out [Defendants'] script." *Id.* Ex. 9 at GUCWA 0023 (16:08:06–16:09:10).

H. Plaintiffs Suffer Loss and Harm by Defendants' Unauthorized Access of the Facebook Website

Facebook became aware of the hacking activities and, as Defendants predicted, tried to prevent Defendants from causing further harm through their continuing to gain unauthorized access into Facebook's computer system. *Id.* Ex. 1 at 241:8-244:1; Ex. 45. Facebook repeatedly instituted measures to stop Defendants' efforts to acquire data from Facebook's site. Rather than stopping the attacks, Defendants re-wrote their code to circumvent Facebook's counter-measures.

For example, in response to the suspected misuse of user emails from Facebook, Zuckerberg modified the code on Facebook's website to block the Social Butterfly programming from loading Facebook's webpages. *Id.* Ex. 1 at 242:7-18. [redacted].[5] Shiflett Decl., ¶¶ 12, 29, 31 & Exs. 1-3. [redacted] *Id.* ¶ 29 & Ex. 1. [redacted] *Id.* [redacted] Cooper Decl. Ex. 32

[5] [redacted] Shiflett Decl., ¶ 31.

at PNS01767 (2/20/2006 entry); Ex. 9 at GUCWA 0098-99 (10:04:59-10:26:43); Ex. 31 at 100:10-103:11, 138:24-141:2, 169:2-182:15; Shiflett Decl. ¶ 30 & Ex. 4 (PNS Source Code) at PNS0281471 [redacted] PNS 0281458. [redacted] Shiflett Decl. ¶ 32 & Ex. 4 at PNS0310219-21; Cooper Decl. Ex. 48 at PNS001334-35 (14:29-14:30).

[redacted][6] Id. Ex. 45; Ex. 9 at GUCWA 0097-0098 (9:36:46-9:52:52); Ex. 31 at 113:22-120:7; Ex. 41 at PNS0281495, PNS0281509 [redacted] PNS0281520, PNS0281522 [redacted], PNS0281504 [redacted]; Shiflett Decl. ¶ 26 & Ex. 4 at PNS0281469 [redacted], PNS0281445, PNS0281456, PNS0281489 (dynacrawl.py v.3), PNS0281496 [redacted]. These text-based user agents, as opposed to web browsers such as Internet Explorer, are commonly used by automated scrapers and, consequently will alert website developers to unauthorized activity.[7] Id. ¶¶ 21, 23. [redacted] Id. ¶¶ 21-23 & Ex. 1 (FBCA051064-101) at [redacted] *Id.* ¶ 24. [redacted] Cooper Decl. Ex. 9 at GUCWA 0098 (09:52:38-10:02:10); Ex. 41 at PNS0281509; Shiflett Decl. ¶¶ 24-26 & Ex. 4 at PNS0281496, PNS0281469.

[redacted]. Shiflett Decl., ¶ 33 & Ex. 2

---

[6] [redacted] When Internet users visit a website, the user-agent generally identifies itself by sending a text string containing the name and version of the user's browser as well as the host operating system. Shiflett Decl. ¶ 21.

[7] Because they are text-based, they do not recognize graphics or photos – integral features of the Facebook website. Shiflett Decl. ¶ 21-23.

(FBCA051102-132) at [redacted]; Cooper Decl. Ex. 1 at 241:8-244:1. [redacted] Shiflett Decl. ¶¶ 34-38; Cooper Decl. Ex. 41 at PNS0281513, PNS0281525.

[redacted] Shiflett Decl. ¶¶ 27-28 & Ex. 4 at PNS0281444, PNS0281459, PNS0281489 [redacted], PNS0281496 [redacted], and Ex. 2 at [redacted]; Cooper Decl. Ex. 41 at PNS0281451, PNS0281453, PNS0281509 [redacted], PNS0281522 [redacted], PNS0281504 [redacted]; Ex. 9 at GUCWA 0049 (16:51:46-16:56:59), GUCWA 0056 (11:48:39-11:50:51, GUCWA 0097 (9:10:17-9:28:10). [redacted] Shiflett Decl. ¶ 28. [redacted] Cooper Decl. Ex. 31 at 101:15-104:20, 105:3-17, 106:11-107:8, 110:15-113:12, 119:9-122:5, 124:19-127:9, 159:23-160:20, 164:13-165:11, 169:2-173:20, 176:20-180:2, 180:11-183:20, 188:24-194:20, 195:3-8; Ex. 9 at GUCWA 0022 (15:16:29-15:18:24), GUCWA 0023 (15:19:07-16:07:54), GUCWA 0056 (11:48:39-11:53:44); Ex. 35 at 148:20-150:16; Shiflett Decl. ¶ 28 & Ex. 4 at PNS 0281444-PNS 0281445.

[redacted] Cooper Decl. Ex. 1 at 243:5-244:19, 248:5-250:13. [redacted]. Cooper Decl. Ex. 1 at 243:5-246:19, 248:5-253:25.

III. ARGUMENT

A. Legal Standard

Under Federal Rule of Civil Procedure 56(c), summary judgment is appropriate if "there is no genuine issue as to any material fact and that the moving party is entitled to a judgment as a matter of law." *Celotex Corp. v. Catrett*, 477 U.S. 317, 322-23 (1986). Once the moving party demonstrates that there is no genuine issue of material fact, the nonmoving party must designate "specific facts showing that there is a genuine issue for trial." *Id.* There is no genuine issue of material fact if "the evidence [ ] is of insufficient caliber or quantity to allow a rational finder of fact" to find for the nonmoving party. *Id.* at 324.

Here, the evidence proves that (1) Defendants knowingly and without permission accessed Facebook's website and engaged in taking, copying, and making use of Facebook's data, and (2) PNS and ConnectU orchestrated a scheme to spam the Facebook user base using invitation emails with false headers sent to addresses illegally harvested from Facebook. Defendants largely admit to engaging in this conduct and simply dispute the legal significance of such acts.[8]

B. Defendants Have Violated California Penal Code § 502(c)

The undisputed evidence shows that Defendants have maliciously violated Penal Code Section 502(c). That statute makes it unlawful for any person to perform the following acts:

> (2) Knowingly accesses and without permission takes, copies, or makes use of any data from a … computer system, … or takes or copies any supporting documentation, whether existing or residing internal or external to a … computer system….
>
> …
>
> (6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.
>
> (7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

Cal. Penal Code § 502(c). Any owner or lessee of the computer, computer system, computer

[8] This Court in its November 30, 2007, Order denying Plaintiffs' Motion for Sanctions indicated "It does not presently appear … that ConnectU disputes the general outline of Facebook's allegations, but ConnectU does vigorously dispute whether any such conduct was wrongful." Doc. No. 231 (11/30/07 Order), at 2 n.1.

network, computer program, or data who suffers damage or loss by reason of a section 502(c) violation can assert this cause of action. Cal. Penal Code § 502(e)(1). Punitive and exemplary damages are allowed when a the defendants' actions constitute oppression, fraud, or malice. Cal. Penal Code § 502(e)(4).

1. **Plaintiffs' Computers Are Covered By Penal Code Section 502(c)**

Section 502(c) is designed to protect computer networks, computer services, and computer systems. There is no dispute that at all times since Facebook's formation, Plaintiffs' computers have comprised a computer system and/or computer network, since the computers contain programs, perform computer services, utilize data storage, and facilitate on-line communication among users. Cooper Decl. Ex. 1 at 84:21-25, 119:6-123:19; 146:5-19, 155:2-156:7, 165:13-166:4; 180:24-181:2; Ex. 2 at 232:19-22, 247:1-250:2; Exs. 3-5; Ex. 49. *See also* Cal. Penal Code § 502(b)(2), (4),(5) (defining "computer network," "computer services," and "computer system").

It also is undisputed that Plaintiffs suffered damage and/or loss as a result of Defendants' actions. Defendants' copying of admittedly millions of email addresses and data that took considerable effort for Facebook to assimilate is precisely the type of loss contemplated by California Penal Code Section 502. The statute was created specifically to expand the degree of protection afforded individuals and businesses "from tampering, interference, damage and unauthorized access," which the Legislature deemed "vital to the protection of the privacy of individuals." Cal. Penal Code § 502(a).

Further, Facebook was forced to engage in efforts to prevent Defendants from gaining further unauthorized access into its network, because of the harm such actions presented. Copper Decl. Ex. 1 at 241:8-244:1; Ex. 45; Shiflett Decl. ¶¶ 20-23, 27, 29, 31, 33 & Exs. 1-3. The harm resulted in significant distraction and management time to modify code on Facebook's website (Cooper Decl. Ex. 1 at 242:7-244:19, 248:5-250:13), [redacted] (Shiflett Decl. ¶¶ 29, 31 & Exs. 1-3) [redacted]

[redacted], (*id.* ¶¶ 15-19 & Ex. 3, Ex. 4 (PNS source code) at PNS0310219-21); [redacted] (*id.* ¶¶ 21-23 and Ex. 1 (Facebook Code) at [redacted] Cooper Decl. Ex. 1 at 242:7-244:19, 248:5-250:13. *See United States v. Middleton,* 231 F.3d 1207, 1213 (9th Cir. 2000) (holding that hours spent fixing computer programs to deal with a computer attack is damage); Cal. Penal Code § 502(b)(9) (defining victim expenditure as time spent assessing damage).

2. Defendants Knowingly and Without Permission Accessed or Caused to be Accessed Facebook's Computer System

This Court already ruled that in determining whether or not Defendants violated Penal Code Section 502(c), it is sufficient for Facebook simply to show that Defendants "knowingly accessed Facebook's website to collect, copy, and use data found thereon in a manner not authorized or permitted by Facebook." *Facebook, Inc. v. ConnectU LLC*, 489 F. Supp. 2d 1087, 1091 (N.D. Cal. 2007). It is undisputed that Defendants conduct satisfies the Court's interpretation of the statute.[9]

Defendants admit that they knowingly accessed Plaintiffs' computers within the meaning of each of Penal Code Section 502(c)(2), (6) and (7). Cooper Decl. Ex. 9 at GUCWA 0022 (15:04:44-15:17:39), GUCWA 0025 (18:28:31-18:44:27), GUCWA 0032-33 (13:23:54-13:28:03), GUCWA 0075-77 (17:28:27-18:19:07); Ex. 10 at 43:12-44:5, 45:17-46:3, 53:6-20; Ex. 11 at 72:17-73:11, 73:19-22, 73:25-74:7; Ex. 7 at 24:10-28:1; Ex. 12 at 31:2-11, 53:22-54:24; Exs. 13-15 at ¶ 2; Exs. 16-18, Responses to Form Interrogatories Nos. 2.11 & 8.2; Ex. 19, Response to Form Interrogatory No. 17.1 at 4-5 (Requests Nos. 2, 9, 10 & 12); Ex. 36; Ex. 25; Ex. 28 at 191:5-192:14; Ex. 21 at 136:12-140:13. Defendants' access was effected by either manually logging into the website using "borrowed" account information or through the use of the automated Facebook Importer and related scripts. *Id.* *See also* Shiflett Decl. ¶¶ 10, 11, 15, 34 & Ex. 4.

---

[9] The Court also already has rejected any argument that Defendants cannot be found liable for violating Penal Code Section 502(c) to the extent Facebook's users did not have any expectation of privacy in the profiles, email addresses, or course information which Defendants harvested. *See Facebook, Inc. v. ConnectU LLC*, 489 F. Supp. 2d at 1091 n.5.

The access to Plaintiffs' computers was without Plaintiffs' permission. "[P]rivate parties [like Facebook] are free to set the conditions on which they will grant … permission" for individuals to access their computer systems. *Facebook, Inc. v. ConnectU LLC*, 489 F. Supp.2d at 1091, n.5. Here, Plaintiffs never authorized Defendants to use third party log-in credentials to sign into the Facebook computer system, or to harvest email addresses and other data. The Terms of Use expressly stated that such conduct was unauthorized. Cooper Decl. Ex. 1 at 238:11-16, 238:22-25, 238:18-239:5; Zuckerberg Decl. ¶¶ 4-10 & Exs. A-C. Defendants exceeded the scope of these Terms of Use, particularly insofar as Defendants collected data for use "in connection with [ConnectU's] commercial endeavors," and insofar as it was actually ConnectU and PNS who accessed Facebook's website. *Id.* Exs. A-C.

Indeed, Defendants knew the access was improper as evidenced by their statements and actions to avoid detection. Cooper Decl. Ex. 9 at GUCWA 0023 (16:07:41-16:09:10), GUCWA 0049 (17:01:22-17:01:25), GUCWA 0076 (17:57:19-17:57:30); Ex. 34 at PNS000015; Ex. 45; Ex. 46; Ex. 47; Ex. 19, Response to Form Interrogatory No. 17.1 at 4-6 (Request Nos. 2, 7, 8, 9, 10, 12, 13 and 15). They learned of complaints that Facebook was being attacked, acknowledged they would need to play "cat and mouse," and discussed how "alarms" were being set off at Facebook. *Id.* As early as 2004, they were told by iMarc that their actions were improper. Cooper Decl. Ex. 21 at 66:4-68:25, 124:23-125:17, 128:13-147:4, 149:9-150:6, 153:13-22, 156:5-157:21; Exs. 22-27. [redacted] *Id.* Ex. 32 at PNS01767 (2/18/2005 entry). [redacted] *See, e.g.*, *id.* Ex. 50.

3. Defendants Admit that They Took, Copied and/or Made Use of Facebook's Data

Defendants also admit that they took, copied and used the data stored on Plaintiffs' computers in violation of Section 502(c)(2). [redacted] Cooper Decl. Ex. 9 at GUCWA 0058 (12:59:42-13:01:03); Ex. 32 at PNS01768 (3/9/05 entry), PNS01769 (4/6/05 entry); Ex. 35 at 148:20-150:16; Ex. 11 at 83:22-84:23, 85:10-87:22; Ex. 36; Ex. 42; Shiflett Decl. ¶¶ 15-16 & Ex. 4 at PNS0281469-73, Ex. 6 at PNS0310177. The undisputed evidence is that millions of addresses and volumes of course information were taken. *Id.* The evidence also shows that Defendants used email addresses copied from the Facebook website to send unsolicited commercial email to Facebook's users inviting them to join ConnectU. *Id.*; *see also, id.* Ex. 51-54.

C. ConnectU and PNS Violated 15 U.S.C. § 7704(a)(1)

ConnectU and PNS also violated the CAN-SPAM Act by initiating commercial email messages that contained materially false or materially misleading header information. 15 U.S.C. § 7704(a)(1).

1. Defendants' Email Messages Are "Commercial" Electronic Mail Messages

The email messages sent by ConnectU are "commercial electronic mail messages" as defined by the Act. An "electronic mail message" is a "message sent to a unique electronic mail address." 15 U.S.C. § 7702(6). A "commercial electronic mail message" is defined as:

> any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service including content on an Internet website operated for a commercial purpose.

15 U.S.C. §7702(2)(A). *See also* 16 C.F.R. 316(3)(a)(1). Commercial electronic mail messages include messages "that may not themselves appear commercial, but that promote a 'commercial service' such as an 'Internet website operated for a commercial purpose.'" 15 U.S.C. § 7704(a)(5)(A); *see also MySpace, Inc. v. Wallac.*, 498 F. Supp. 2d 1293, *15 (C.D. Cal. 2007) (although the website in question did not request money from visitors, Defendant admitted his business was commercial venture); *Aitken v. Commc'n Workers of America,* 496 F. Supp. 2d 653, 662 (E.D. Va. 2007) (holding that unsolicited emails seeking membership in an organization such

as a union are "commercial electronic mail messages.").

The messages speak for themselves as commercial promotion of ConnectU.com.

2. ConnectU and PNS "Initiated" the Transmission of the Emails

ConnectU and PNS "initiated" transmission of the commercial emails. *See* 15 U.S.C. § 7704(a)(1); 15 U.S.C. § 7704(b)(1)(A); 15 U.S.C. § 7702(9). *See also* 15 U.S.C. § 7706(g)(2) (defining "procure"). ConnectU sent unsolicited emails from "bogus" email addresses on July 22, 2004. Cooper Decl. Ex. 26; Ex. 19 Response to Form Interrogatory 17.1, at 5 (Request No. 8); Ex. 21 at 140:14-147:4. In addition, ConnectU's principals, Cameron and Tyler Winklevoss, personally oversaw all aspects of the design and operation of the software programs. *See, e.g.,* Ex. 19 Response to Form Interrogatory 17.1, at 5-6 (Request Nos. 12-13); Ex. 30 at 19:14-20:9; Ex. 11 at 32:11-33:16, 35:15-23, 82:2-83:2 [redacted]. *Id.* Ex. 31 at 57:24-60:2, 72:2-73:20, 86:8-89:14, 165:12-17, 167:22-168:3; Ex. 30 at 27:24-28:6, 98:2-99:3, 104:5-8, 106:13-18, 172:4-16; Ex. 32; Ex. 33; Ex. 34 at PNS000015; Ex. 35 at 148:20-151:6, 29:17-31:23; Ex. 11 at 83:22-84:23, 85:10-87:22; Ex. 36. Specifically, David Gucwa and Wayne Chang were hired by ConnectU to develop a "social network spider," which became Importer, Crawler and Social Butterfly, to copy email addresses and send to those email addresses "unsolicited commercial emails." Cooper Decl. Ex. 9 at GUCWA 0057 (12:02:45-12:06:49); Ex. 34; Ex. 36; Ex. 55; Ex. 56 at 4:23-24.

Defendant PNS also implemented ConnectU's directive. According to Cameron Winklevoss, PNS "was involved in creating and implementing an automated process for sending invitations to various email addresses found on facebook.com." *Id.* Ex. 56 at 4:23-24. [redacted] *Id.* Ex. 41 at PNS0296805-06; Ex. 30 at 154:15-155:7, 158:3-7; Ex. 57 at 309:12-318:12. They were sent and paid for by ConnectU under the direction of John Taves, a PNS principal, who was deeply involved in the operation of Social Butterfly. *Id.* Ex. 30 at

150:11-16. [redacted] *Id.* Ex. 30 at 147:20-155:7. [redacted] *Id.* Ex. 30 at 150:11-153:10 Ex. 58; Ex. 59; Ex. 45; Ex. 46. [redacted] *E.g., id.*, Ex. 41 at PNS0320945 & Shiflett Decl. Ex. 4 at PNS0310221. [redacted] Cooper Decl. Ex. 30 at 45:14-49:12, 65:9-69:13. Williams actively participated in every stage of Social Butterfly's development and maintained its steady operation. *Id.* Ex. 11 at 85:22-87:3; Ex. 35 at 148:20-151:3; Ex. 60 at 5:19-6:14; Ex. 19 Response to Form Interrogatory 17.1, at 5-6 (Request Nos. 12-13). Williams also directly oversaw and controlled the operation of the importer. *Id.* Ex. 61. [redacted] *Id.* Ex. 42.

3. The Emails Sent by PNS and ConnectU Had False Headers

The email headers did not identify the source of the emails as ConnectU. Rather, they used false names or names of third parties. Falsifying the "from" line in commercial email in this manner is "materially false or materially misleading" because it is likely to affect the recipient's opinion of the value of the service advertised. *Aitken, et al. v. Commc'n Workers of America, et al.*, 496 F. Supp. 2d 662 (E.D.Va. 2007). In *Aitken,* Verizon Business Network Services asserted a Section 7704(a)(1) claim against a union organization for sending materially false and misleading commercial emails to Verizon employees. The union created Yahoo email addresses that contained the names of Verizon managers, and sent unsolicited emails from those addresses to Verizon workers. *Id.* at 655. The emails disparaged Verizon and touted the benefits of unionization. *Id.* The Court found that the messages "might have more credibility coming from a putative Verizon manager than an outsider" and, therefore, the misleading "from" address alone may have "affected an objective recipient's opinion of the value of joining [the union]." *Id.* at 667. The Court noted that a "material fact under the Act is one 'likely to affect a consumer's choice . . . regarding a product. In other words, it is information important to consumers.'" *Id.*

(*quoting* 70 Fed. Reg. at 3315). The Court ruled that this deceptive practice supported a 7704(a)(1) claim and denied a motion to dismiss the claim. *Id.*

By sending email purporting to come from a friend known to the recipient when in fact they originated with ConnectU, Defendants' actions are strikingly similar to those at issue in *Aitken.* [redacted] Cooper Decl. Ex. 40; Ex. 43. Believing that an email came from a friend rather than an unknown company is "likely to affect" the recipient's evaluation of the content of the email. *See also* 70 Fed. Reg. at 3315. In addition, the false senders were individuals who were designated as the recipients' friends on Facebook, a social networking website in direct competition with the website advertised in the emails. The false senders therefore are known to the recipients to have experience with social networking websites. Email from these friends concerning a competing social networking website would have more credibility than the same emails coming from an outsider or a company.

In addition, to using fake headers with real people's names, ConnectU and PNS sent numerous emails from fabricated addresses that did not even exist, including "god@harvard.edu." They also used the name "jstarr" with multiple fake ".edu" addresses. *Id.* Ex. 29. Each of these also was a false header under the CAN-SPAM Act.

4. Defendants' Actions Constitute an Aggravated Violation Allowing for Trebling

Plaintiffs are entitled to treble damages under Section 7704(g). Under Section 7704(g), trebling is appropriate in two circumstances: (1) if the violation was willful and knowing or (2) if the emails were harvested by automated means as set forth in Section 7704(b)(1). *See* § 7704(b)(1) (describing aggravated offense). Both criteria are met.

a. ConnectU and PNS's Actions Were Willful and Knowing.

ConnectU had actual knowledge that the commercial emails violate the Act. [redacted]

[redacted] *Id.* Ex. 29. [redacted] *Id.* [redacted] *Id.* Nevertheless, ConnectU continued its spamming campaign.

PNS also had actual knowledge that the commercial emails violate the Act. [redacted] *Id.* [redacted] *Id.* Ex. 34 at PNS000015 (emphasis added).

b. ConnectU and PNS' Automated Harvesting Violated Section 7704(b)(1).

Defendants' knowing use of automated programs to harvest the email addresses to which the commercial emails were sent, together with Defendants' actions in violation of Section 7704(a)(1), constitutes an aggravated violation of Section 7704(a)(1). Section 7704(b)(1) provides as follows:

> (A) IN GENERAL. -- It is unlawful for any person to initiate the transmission, to a protected computer, of a commercial electronic mail message that is unlawful under subsection [7704](a), or to assist in the origination of such message through the provision or selection of addresses to which the message will be transmitted, if such person had actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that—
>
> (i) the electronic mail address of the recipient was obtained using an automated means from an Internet website or proprietary online service operated by another person, and such website or online service included, at the

> time the address was obtained, a notice stating that the operator of such website or online service will not give, sell, or otherwise transfer addresses maintained by such website or online service to any other party for the purposes of initiating, or enabling others to initiate, electronic mail messages[.]

15 U.S.C. § 7704(b)(1)(A)(i).

As extensively detailed in the Factual Background, ConnectU and PNS harvested e-mail addresses from Facebook and generated commercial emails to addresses obtained via the automated means. Defendants cannot dispute that they knew the email addresses to which spam emails were sent were obtained via automated means, *i.e.*, the software programs they wrote and revised over the course of months. Indeed, automation was the goal of writing and continually revising the programs to circumvent Facebook's security measures.

The Facebook Website also contained the required notice under 7704(b)(1). Between February 4, 2004 and August 2005, Facebook's Privacy Policy specified that "Email addresses will never be sold to anyone, and they will not be used for spam or any other purpose outside of the site itself." Zuckerberg Decl. ¶ 8 & Exs. D-E. In addition, Facebook's Terms of Use for this period precluded (a) using the site for commercial endeavors, (b) "harvesting" of email addresses and other profile information of registered users, (c) use of the site by companies "for any purpose" and (e) collecting of email addresses from Facebook "for the purpose of sending unsolicited email." *Id.* ¶ 4 & Exs. A-C. These notices more than satisfy the Section 7704 (b)(1)(A)(1) requirement of "a notice stating that the operator of such website . . . will not give, sell, or otherwise transfer addresses maintained by such website . . . to any other party for the purposes of initiating, or enabling others to initiate, electronic mail messages."

D. Facebook and Zuckerberg Were Adversely Affected

The Act authorizes any "provider of Internet access service adversely affected" by violations of sections 7704(a)(1) or 7704(b) of the Act to bring a civil action. 15 U.S.C. § 7706(g)(1); *see also* Cooper Decl., Ex. 62 at 21 (emphasis added) ("Section 7(f) [now 15 U.S.C. § 7706(g)] would allow a provider of Internet access service adversely affected by a violation of section 5 [15 U.S.C. § 7704] to bring a civil action in Federal district court or other court of competent jurisdiction. This could include a service provider who carried unlawful spam over its facilities, or who operated a website or online service from which recipient email addresses were harvested in connection with a violation of section [7704](b)(1)(A)(i))"). For the same reasons set forth with respect to the harm suffered by plaintiffs, Facebook and Zuckerberg were adversely affected by ConnectU and PNS' actions.

IV. CONCLUSION

Based upon this undisputed evidence, plaintiffs request a summary judgment finding of a willful violation of California Penal Code section 502(c) and aggravated violations of 15 U.S.C. §§ 7704(a)(1) and 7704(b)(1).

Dated: January 7, 2008

ORRICK, HERRINGTON & SUTCLIFFE LLP

/s/ I. Neel Chatterjee /s/

I. Neel Chatterjee
Attorneys for Plaintiffs
THE FACEBOOK, INC. and MARK ZUCKERBERG

CERTIFICATE OF SERVICE

I hereby certify that this document(s) filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF) and paper copies will be sent to those indicated as non registered participants on January 7, 2008.

Dated: January 7, 2008.

Respectfully submitted,

/s/ I. Neel Chatterjee /s/
I. Neel Chatterjee

OHS West:260364214.1
16069-4